IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

NANCY MURPHY and ROBERT STEWART, **Plaintiffs,** **v.** **THOMAS JEFFERSON UNIVERSITY HOSPITALS INC. d/b/a JEFFERSON HEALTH** **Defendant.**	**Case No. 22-cv-4674-BMS** **JURY TRIAL DEMANDED**

SECOND AMENDED CLASS ACTION COMPLAINT

Nancy Murphy and Robert Stewart ("Plaintiffs"), individually and for all others similarly-situated, by and through their undersigned counsel, bring this action against Thomas Jefferson University Hospitals, Inc. d/b/a Jefferson Health ("Jefferson Health" or "Defendant"), alleging as follows:

NATURE OF THE ACTION

1. Plaintiffs bring this action for themselves and thousands of other patients whose medical privacy has been violated by Jefferson Health's use of Meta Platform Inc.'s ("Meta") tracking and collection tools, including the Meta Pixel, Meta SDK, Meta Conversions API, customer list uploads, social plug-ins, the Meta Graph API, server-to-server transmissions, and all similar collection tools (collectively, "Meta Collection Tools"). The Meta Collection Tools allow Jefferson Health to intercept individually-identifiable health information from Jefferson Health's web properties and monetize this information for its own financial gain.

2. Meta operates the world's largest social media company. Meta's revenue is derived almost entirely from selling targeted advertising. Meta's "Health" division is dedicated to marketing to and servicing Meta's healthcare "Partners." Meta defines its "Partners" to include

"businesses" that use Meta's products, including the Meta Pixel or Meta Audience Network tools "to advertise, market, or support their products and services."

3. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

4. Plaintiffs are Jefferson Health patients who allege that Jefferson Health installed the Meta Collection Tools on its website (*www.jeffersonhealth.org*), the MyJeffersonHealth online portal, and the MyJeffersonHealth Mobile Application ("Jefferson Health's web properties") to share their confidential health information with Meta for financial gain in violation of federal and state laws, and despite Defendant's express promise that: "We will obtain your written permission when the uses and disclosures of PHI are for marketing purposes or other activities where we receive remuneration in exchange for disclosing such PHI." *See* Jefferson Health Notice of Privacy Practices *https://www.jeffersonhealth.org/privacy-practices*.

5. When a patient uses Jefferson Health's web properties where Meta Collection Tools are present, the Meta Collection Tools transmit the content of their communications to Meta, including, but not limited to: (1) signing-up for a patient portal; (2) signing-in or -out of a patient portal; (3) taking actions inside a patient portal; (4) making, scheduling, or participating in appointments; (5) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; (6) conduct a search on Jefferson Health's web properties; and (7) other information that qualifies as "personal health information" under federal and state laws.

6. Meta Collection Tools also collect and transmit information from Jefferson Health that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Meta encourages its healthcare Partners to use to upload customer lists to Meta for use in its advertising systems. In the case of Jefferson Health, a customer list is a patient list.

7. The information transmitted from Jefferson Health's web properties to Meta always includes information sufficient to uniquely identify a patient under federal law (such as IP address information and device identifiers that Meta associates with a patient's Meta account), and may also include a patient's demographic information, email address, phone number, computer ID address, or contact information entered as emergency contacts or for advanced care planning, along with information like appointment type and date, a selected physician, button and menu selections, the content of buttons clicked and typed into text boxes, and information about the substance, purport, and meaning of patient requests for information from Jefferson Health under federal and state health privacy laws.

8. The transmission of this information is instantaneous, invisible, and occurs without any notice to the patient that it is occurring.

9. Meta collects the transmitted identifiable health information and uses "cookies" to match it to Facebook users, allowing Jefferson Health to target advertisements both on and off Facebook. For example, Jefferson Health and Meta can target ads to a person who has used a patient portal and exchanged communications about a specific condition, such as cancer.

10. Instead of taking proactive steps to verify that businesses using Meta Pixels obtain the required consent, Meta uses an "honor system" under which Meta assumes these businesses "represent and warrant that [they have] provided robust and sufficient prominent notice to users

regarding the Business Tool Data collection, sharing, and usage." *See* Facebook Business Tools Terms, *https://www.facebook.com/legal/terms/businesstools*.

11. The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104-191, 110 Stat. 1936 (1996) and Pennsylvania's law relating to the confidentiality of medical records, 28 Pa. Code § 115.27, both prohibit healthcare providers from sharing health care information, medical records, and related information with third parties except as needed for a patient's treatment, payment, or with their consent. Importantly, these laws give patients a reasonable expectation of privacy in communications with healthcare providers relating to their medical conditions and treatment, because this information may not be disclosed outside the healthcare setting without notice and consent.

12. The United States Department of Health and Human Services ("HHS") recently confirmed that HIPAA and its regulations prohibit the transmittal of individually-identifiable health information by tracking technology like the Meta Pixel without the patient's authorization and other protections like a business associate agreement with the recipient of patient data.[1]

13. Meta's Terms of Service, Data Policy, and Cookies Policy neither inform Facebook users that Meta may acquire their health information when they interact with healthcare providers' websites and applications, nor obtain their consent for any such acquisitions.

14. Jefferson Health's interception, dissemination, and use of individually-identifiable health information not only violates federal and state law but also harms patients by intruding upon their privacy; erodes the confidential nature of the provider-patient relationship; and takes patients' property and property rights without compensation and ignores their right to control the

[1] *See* Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates, *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

dissemination of their health information to third parties. In addition, Jefferson Health has been unjustly enriched by its misconduct, obtaining unearned revenues derived from its unauthorized disclosure of patient information.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 over the claims that arise under the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq*.

16. This Court also has subject-matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d), which, under the Class Action Fairness Act of 2005, 28 U.S.C. §§ 1332(d), 1453 and 1711-15 ("CAFA"), expressly provides federal courts with jurisdiction over any class action in which: the proposed class includes at least 100 members; any member of the class is a citizen of a state and any defendant is a citizen or subject of a foreign state; and the amount in controversy exceeds $5,000,000.00, exclusive of interest and costs.

17. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because Defendant does business in, and is subject to, personal jurisdiction in this District. Venue is also proper in this District, because a substantial part of the events or omissions giving rise to the claim occurred in, and emanated from, this District.

MATERIAL FACTS

Meta's Collection Tools Redirect Patients' Data From Jefferson Health's Web Properties To Use For Ad Targeting

18. Meta maintains profiles of its Facebook users that include the users' real names, locations, email addresses, friends, "likes," and communications.

19. Meta associates this information with personal identifiers, including IP addresses, cookies, and device identifiers.

20. Meta also tracks non-users across the web through its widespread Internet marketing products and source code, including the Meta Pixel.

21. Meta's revenue is derived almost entirely from selling targeted advertising, which includes, but is not limited to, targeted advertising to Meta properties and to all Internet users on non-Meta sites and apps.

22. Meta's Business division provides advertising services and tools to web developers, including the Meta Collection Tools. Meta's Business division and its advertising services and tools are focused on trade and commerce.

23. The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their website to "measure, optimize and build audiences for … ad campaigns."[2]

24. Meta describes the Pixel as "a snippet of JavaScript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook User accounts.[3]

25. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[4]

26. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. "measure cross-device conversions" and "understand how your cross-device ads help influence conversion.";

[2] Meta, Meta Pixel (2023), *https://www.facebook.com/business/tools/meta-pixel.*
[3] Meta for Developers, Meta Pixel (2023), *https://developers.facebook.com/docs/meta-pixel/.*
[4] Meta, Meta Pixel (2023), *https://www.facebook.com/business/tools/meta-pixel.*

b. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

c. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[5]

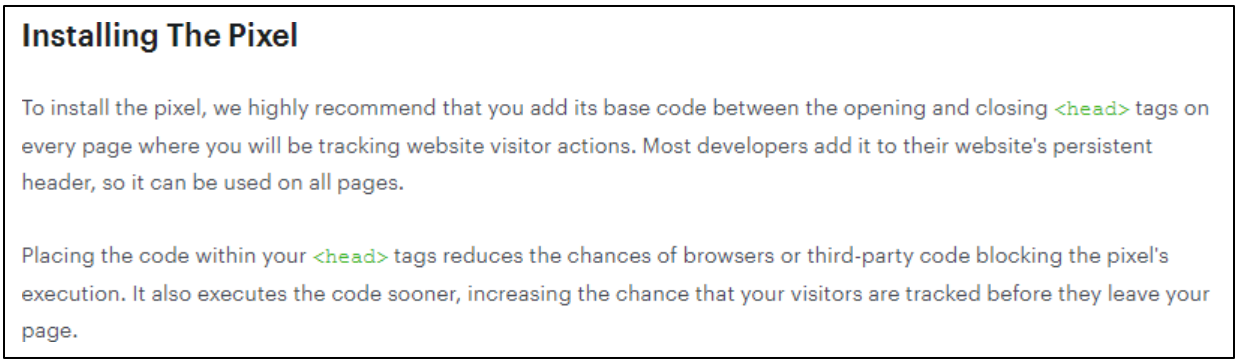
27. Meta explains that the Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

28. The Meta Pixel is customizable. Web developers can choose the actions the Pixel will track and measure.

29. Meta advises web developers to place the Pixel early in the source code for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website:[6]

[5] *Id.*
[6] Meta For Developers, Get Started (2023), *https://developers.facebook.com/docs/meta- pixel/get-started.*



Installing The Pixel

To install the pixel, we highly recommend that you add its base code between the opening and closing <head> tags on every page where you will be tracking website visitor actions. Most developers add it to their website's persistent header, so it can be used on all pages.

Placing the code within your <head> tags reduces the chances of browsers or third-party code blocking the pixel's execution. It also executes the code sooner, increasing the chance that your visitors are tracked before they leave your page.

30. Meta also provides advertisers with step-by-step instructions for setting up and installing the Meta Pixel on their website, so that companies can add the Meta Pixel to their website without a developer.[7]

31. If a healthcare provider, such as Jefferson Health, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta. When a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with her healthcare provider. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it.

32. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing."[8]

33. Jefferson Health discloses the content of the communication to Meta while the patient is exchanging the communication with Jefferson Health's web properties.

---

[7] Meta, Meta Pixel (2023), *https://www.facebook.com/business/tools/meta-pixel.*

[8] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything*, USA Today (March 4, 2020 4:52 am), *https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/#.*

Meta Uses Identifiers To Match The Health Information It Collects With Facebook Users

34. Meta uses cookies to identify patients, including cookies named c_user, datr, fr, and _fbp.

35. The c_user cookie identifies Facebook users. The c_user cookie value is the Facebook equivalent of a user identification number. Each Facebook user account has one – and only one – unique c_user cookie. Meta uses the c_user cookie to record user activities and communications.

36. An unskilled computer user can obtain the c_user cookie value for any Facebook user by (1) going to the user's Facebook page, (2) right-clicking with their mouse, (3) selecting "View page source," (4) executing a control-f function for "UserID," and (5) copying the number value that appears after "UserID" in the page source code of the Facebook user's page.

37. Following these directions makes it possible to discover that the Facebook UserID assigned to Mark Zuckerberg is 4. By typing *www.facebook.com/4* into a browser and hitting enter, a browser directs to Mr. Zuckerberg's page at *www.facebook.com/zuck*.

38. The Meta datr cookie identifies the web browser the patient is using. It is an identifier unique to each patient's specific web browser, so is another way Meta can identify Facebook users.

39. Meta keeps a record of every datr cookie identifier associated with each of its users, and a Facebook user can obtain a redacted list of all datr cookies associated with his or her Facebook account from Meta by using the Facebook "Download Your Information" tool.

40. The Meta fr cookie is an encrypted combination of the c_user and datr cookies.[9]

41. The c_user, datar, and fr cookies are traditional third-party cookies, meaning they are cookies associated with a party other than the entity with which a person is communicating at the time. In the case of Jefferson Health, they are third-party cookies because Meta is a third-party to the communication between a patient and their healthcare provider.

42. The Meta _fbp cookie is a Facebook identifier that is set by Facebook source code and associated with the healthcare provider using the Meta Pixel.

43. The letters fbp are an acronym for Facebook Pixel.

44. The _fbp (or Facebook Pixel) cookie is also a third-party cookie in that it is also a cookie associated with Meta that is used by Meta to associate information about a person and their communications with non-Meta entities while the person is on a non-Meta website or application.

45. Meta disguises the _fbp cookie as a first-party cookie even though it is Meta's cookie on non-Meta websites.

46. By disguising the _fbp cookie as a first-party cookie for a healthcare provider rather than a third-party cookie associated with Facebook, Meta ensures that the _fbp cookie is placed on the computing device of patients who seek to access the patient portal.

47. Healthcare providers with a patient portal require patients to enable first-party cookies to gain access to their patient records through the portal.

48. The purpose of these portal-associated first-party cookies is security. The _fbp cookie is then used as a unique identifier for that patient by Meta. If a patient takes an action to

[9] *See* Gunes Acar, *et al.*, Facebook Tracking Through Social Plug-ins: Technical Report Prepared for the Belgian Privacy Commission (Mar. 27, 2015), *https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.*

delete or clear third-party cookies from their device, the _fbp cookie is not impacted – even though it is a Meta cookie – again, because Meta has disguised it as a first-party cookie.

49. Meta also uses IP address and user-agent information to match the health information it collects from Meta healthcare Partners with Facebook users.

Meta Encourages Healthcare Partners, Including Jefferson Health, To Upload Patient Lists For Ad Targeting

50. Meta offers an ad targeting option called "Custom Audiences." When a patient takes an action on a Meta healthcare Partner's website embedded with the Pixel, the Pixel will be triggered to send Meta "Event" data that Meta matches to its users. A web developer can then create a "Custom Audience" based on Events to target ads to those patients. The Pixel can then be used to measure the effectiveness of an advertising campaign.[10]

51. Meta also allows Meta healthcare Partners to create a Custom Audience by uploading a patient list to Meta. As Meta describes it:[11]

> A Custom Audience made from a customer list is a type of audience you can create to connect with people who have already shown an interest in your business or product. It's made of information - called "identifiers" - you've collected about your customers (such as email, phone number and address) and provided to Meta. Prior to use, Meta hashes this information.
>
> Then, we use a process called matching to match the hashed information with Meta technologies profiles so that you can advertise to your customers on Facebook, Instagram and Meta Audience Network. The more information you can provide, the better the match rate (which means our ability to make the matches). Meta doesn't learn any new identifying information about your customers.

[10] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*; *see also,* Meta Blueprint, Connect your data with the Meta Pixel and Conversion API (2023), *https://www.facebookblueprint.com/student/activity/212738?fbclid=IwAR3HPO1d_fnzRCUAhKGYsLqNA-VcLTMr3G_hxxFr3GZC_uFUcymuZopeNVw#/page/5fc6e67d4a46d349e9dff7fa*

[11] Meta Business Help Center, *About Customer List Custom Audiences* (2023), *https://www.facebook.com/business/help/341425252616329?id=2469097953376494*.

52. Meta provides detailed instructions for healthcare Partners to send their patients' individually-identifiable information to Meta through the customer list upload. For example:

> **Prepare your customer list in advance.** To make a Custom Audience from a customer list, you provide us with information about your existing customers and we match this information with Meta profiles. The information on a customer list is known as an "identifier" (such as email, phone number, address) and we use it to help you find the audiences you want your ads to reach.
>
> Your customer list can either be a CSV or TXT file that includes these identifiers. To get the best match rates, use as many identifiers as possible while following our formatting guidelines. You can hover over the identifiers to display the formatting rules and the correct column header. For example, **first name** would appear as **fn** as a column header in your list.
>
> Alternatively, we have a file template you can download to help our system map to your identifiers more easily. (You can upload from Mailchimp as well.)

53. Meta healthcare Partners can then use the Custom Audiences derived from their patient list with the Pixel and Pixel Events for Meta marketing campaigns and to measure the success of those campaigns.

Jefferson Health Sends A Broad Spectrum Of Identifiable Health Information To Meta Through The Meta Collection Tools

54. The information Jefferson Health sends to Meta from its use of the Meta Collection Tools includes, but is not limited to, the following:

a. when a patient clicks to register for a provider's patient portal;

b. information that a patient types into registration forms;

c. when a patient clicks to log in to the patient portal;

d. when a patient clicks to log out of the patient portal;

e. when a patient sets up or schedules an appointment;

f. information that a patient types into an appointment form;

g. when a patient clicks a button to call the provider from a mobile device directly from the provider's website;

h. descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

i. the communications a patient exchanges through Jefferson Health's web properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including whether they are made while a patient is still logged in to a patient portal or around the same time that the patient has scheduled an appointment, called the medical provider, or logged in or out of the patient portal; and

j. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

55. Jefferson Health's conduct constitutes an egregious breach of social norms as demonstrated by public polling that shows: "[n]inety-seven percent of Americans believe that doctors, hospitals, labs, and health technology systems should not be allowed to share or sell their sensitive health information without consent.[12]

Plaintiffs' Allegations Include Jefferson Health's Use Of Meta's Other Collection Tools And Both Website And Applications

56. Defendant's use of Meta's Collection Tools on its web-properties caused the interception and disclosure to Meta of thousands of Jefferson Health patients' individually-identifiable health information.

57. Jefferson Health collects patients' health information on its websites and applications using the same technology, namely JavaScript source code that commands a patient's browser or application to re-direct Event Data through the HTTPS protocol to Meta at a Meta

[12] *Poll: Huge majorities want control over health info,* Healthcare Finance (Nov. 10, 2020), *https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info.*

"endpoint," *i.e.*, a URL at a domain controlled by Meta that exists for the purpose of acquiring such information.

58. Jefferson Health also uses the Meta Pixel in mobile "hybrid" applications. A hybrid application is created using identical source code and language to display a web-property on an application or through a website on a browser application. The benefit of a hybrid application is that identical source code can be used across all web-properties – *i.e.*, a website, an Android application, and an iOS application. Meta provides source code for "hybrid apps" and states that its code "convert[s] Facebook Pixel events into App events."

59. Meta combines health information on specific persons across different devices and different Meta endpoints. Meta can—and does—associate health information with individual patients gathered across different devices and across different healthcare provider web properties, including both websites and applications.

60. Meta's "Consolidated Container" for Event Data – the Meta Conversions API – "enables advertisers to send web, app, and physical store events to Meta through a single endpoint rather than across multiple sources."[13] This consolidation will "simplify an advertiser's tech stack and create a more comprehensive view within Meta Events Manager by using data sets." *Id.* In addition, "App Events" can be "associated with a dataset" through which Meta "connects… event data from web, app, and store event sources to the conversions API." *Id.* The data Meta collects "may show event data from any of these integrations…, including website, app, and offline events." *Id.* As a result, "all customer activities" can be viewed "from a single interface" in a single storage location that Meta calls a "consolidated container." *Id.*

[13] Meta for Developers, *Conversions API for App events* (2023), *https://developers.facebook.com/docs/marketing-api/conversions-api/app-events/*.

61. The Facebook SDK, specifically, "can automatically log app installs, app sessions, and in-app purchases" when deployed on a healthcare provider application.[14] The Facebook SDK can also be used to log other events that users take on an application.

62. Meta's "Graph API is the primary way to get data into and out of the Facebook platform." It is based on Meta's concept of a social graph, which is a "representation of the information on Facebook" which is "composed of nodes, edges, and fields."[15]

63. Through server-to-server transmissions, developers "can share data directly [with Meta] from [their] server, rather than through a browser."[16]

64. When a HIPAA-covered entity, like Jefferson Health, installs the Pixel, SDK, and Conversions API on both its website and application, Meta collects Event Data from the website and the application, places it in a consolidated container, uses the comingled information, and sends the results back to the entity.

Jefferson Health Violates Its Own Privacy Policy & Promises

65. To attract patients, enable their pursuit of medical care, foster its provision of that medical care, and support its business, the Jefferson Health web properties enable individual patients to engage in a wide array of communications concerning their individually-identifiable health information.

66. With respect to patients' individually-identifiable patient health information, Jefferson Health's Patient Rights & Responsibilities advises that patients: "have the right to… discuss your care in places designed to protect your privacy… [and] [e]xpect all communications

[14] *https://developers.facebook.com/docs/app-events/overview.*
[15] *https://developers.facebook.com/docs/graph-api/overview.*
[16] *https://developers.facebook.com/docs/marketing-api/conversions-api/guides/end-to-end-implementation/*

and records related to care, including who is paying for your care, to be treated as private." *See* Jefferson Health Patient Rights & Responsibilities, *https://www.jeffersonhealth.org/your-health/patients-guests/patient-rights-responsibilities/patient-rights-statement*.

67. With respect to patients' individually-identifiable patient health information, Jefferson Health's Notice of Privacy Practices represents that "Jefferson Health understands that information about you and your health is very personal. Therefore, we strive to protect your privacy. We are required by law to maintain the privacy of our patients' protected health information." *See* Jefferson Health Notice of Privacy Practices *https://www.jeffersonhealth.org/privacy-practices*.

68. With respect to patients' individually-identifiable patient health information, Jefferson Health's Notice of Privacy Practices represents that "We will obtain your written permission when the uses and disclosures of PHI are for marketing purposes or other activities where we receive remuneration in exchange for disclosing such PHI." *Id*.

69. With respect to patients' individually-identifiable patient health information, Jefferson Health's Notice of Privacy Practices represents that "Should we wish to disclose your PHI in any manner that would constitute a sale of your PHI, we will obtain your written authorization to do so." *Id*.

70. With respect to patients' individually-identifiable patient health information, Jefferson Health's Online Privacy Statement represents that:

> *You may visit our website without submitting any information about yourself*. If you send us e-mail or subscribe to one of our on-line publications, you will be asked to submit information about yourself. We will use this information for replying to your message or forwarding the requested material. *We do not share this information with any other partners, affiliates or members of JHS. Our website may log the IP addresses of visitors, but only to*

> *administer the site and diagnose problems with our server. IP addresses are not used to identify individuals*.

See Jefferson Health Online Privacy Statement, *https://www.jeffersonhealth.org/privacy-practices /online-privacy-statement*.

71. Notwithstanding all these representations, Jefferson Health designed the Meta Collection Tools to capture both the "characteristics" of individual patients' communications with the Jefferson Health website (*i.e.*, their IP addresses, Facebook ID, cookie identifiers, device identifiers and account numbers) and the "content" of these communications (*i.e.*, the buttons, links, pages, and tabs they click and view).

72. Notwithstanding all these representations, Jefferson Health installed Meta's Collection Tools on its website and, thereafter, began to automatically receive extensive individually-identifiable patient health information from everyone who visited the website.

73. As an example, anyone who visits Jefferson Health's website and clicks on the "Conditions & Treatments" tab is directed to a page, *https://www.jeffersonhealth.org/conditions-and-treatments*, showing 497 different conditions, tests, and treatment options, ranging from "24-Hour Ambulatory pH Monitoring" to "Zenker's Diverticulum." Someone who clicks the "Breast Cancer" button is directed to a page, *https://www.jeffersonhealth.org/conditions-and-treatments/breast-cancer*, which includes buttons and links that provide information about specific treatment options, services, locations, and frequently asked questions, each with a separate link. Selecting any of these links, like "See Treatment Options" directs them to a new page, like *https://www.jeffersonhealth.org/conditions-and-treatments/breast-cancer/treatments-we-offer*, which includes more buttons linked to specific breast cancer treatments. Someone who clicks on "Chemotherapy" is directed to an additional page, *https://www.jeffersonhealth.org/conditions-*

and-treatments/chemotherapy, providing information about chemotherapy, treatment options, services, providers, locations, and clinical trials, many of which have additional links and buttons.

74. The Meta Collection Tools intercept both the "characteristics" and "content" of all these communications with Jefferson Health's web properties, including individually-identifiable patient health information (*i.e.*, about cancer care, breast cancer, chemotherapy treatment, and breast cancer clinical trials) and automatically transmits this data to Meta.

75. After receiving individually-identifiable patient health information communicated on Jefferson Health's web properties, Meta analyzes and uses this information for its own commercial purposes that include building more fulsome profiles of its users' preferences and traits, and selling more-targeted advertisements based on this information. Meta also receives an additional commercial benefit from Jefferson Health's use of Meta's Collection Tools, namely that it provides Jefferson Health with a greater incentive to advertise on Meta's social media platforms.

76. After receiving individually-identifiable patient health information communicated on the Jefferson Health's web properties, Meta forwards this data, and its analysis of this data, to Jefferson Health. Jefferson Health then uses this data and analysis for its own commercial purposes that include understanding how people use its website and determining what ads people see on its website. Jefferson Health also receives an additional commercial benefit from using Meta's Collection Tools, namely that grants Meta access to the commercially-valuable, individually-identifiable patient health information communicated on its web properties.

77. Meta is not an intended recipient of the individually-identifiable patient health information communicated on Jefferson Health's web properties, nor is it an active or disclosed participant in these communications.

78. Jefferson Health does not notify users of its web properties that it is automatically sending individually-identifiable patient health information communicated on its web properties to Meta.

79. Jefferson Health does not notify users of its web properties that individually-identifiable patient health information they communicate on its web properties is being used by Meta for commercial purposes.

80. Jefferson Health does not notify users of its web properties that it is using the individually-identifiable patient health information they communicate on its web properties for commercial purposes.

81. Meta has not secured any informed consent or written permission allowing it to use individually-identifiable patient health information communicated on Jefferson Health's web properties for commercial purposes.

82. Jefferson Health has not secured any informed consent or written permission allowing it to share individually-identifiable patient health information communicated on its web properties with Meta.

83. Jefferson Health has not secured any informed consent or written permission allowing it to use individually-identifiable patient health information communicated on its web properties for commercial purposes.

Meta Falsely Promises Facebook Users That It Requires Healthcare Partners To Have The Right To Share Their Data

84. Every Facebook user is legally deemed to have agreed to the Terms of Service, Data Policy/Privacy Policy, and Cookie Policy via a checkbox on the sign-up page. The Terms of Service, Data Policy/Privacy Policy, and Cookie Policy are binding on Meta and its users.

85. The Meta contract documents contain general statements that, in exchange for the use of Meta's services, Meta will generally collect information about Facebook users.

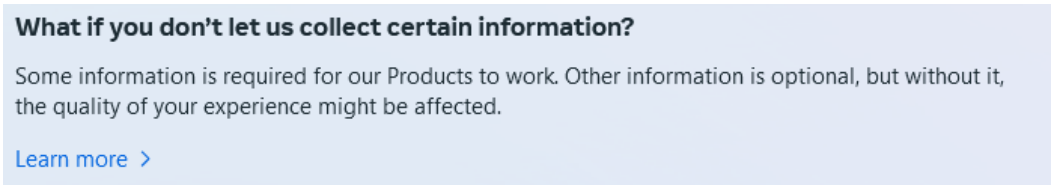
86. Meta does not charge users any money to use its services, but Meta is not "free."

87. In 2019, Meta removed language on its webpage that stated, "It's free and always will be."[17] This conduct demonstrates that using Meta is not, in fact, free. As a digital law expert has explained: "Facebook is not free nor has it ever been. Facebook's currency was and still is its users' personal data. It's never been free, though, because data is worth a lot of money." *Id.*

88. Rather than making users pay money out-of-pocket to use Facebook, Meta makes them pay for its services by allowing Meta to collect some types of personal data under a "data license."

89. Meta's contract states, "We collect and use your personal data in order to provide the services described above to you." It then informs users, "You can learn how we collect and use your data in our Data Policy."[18]

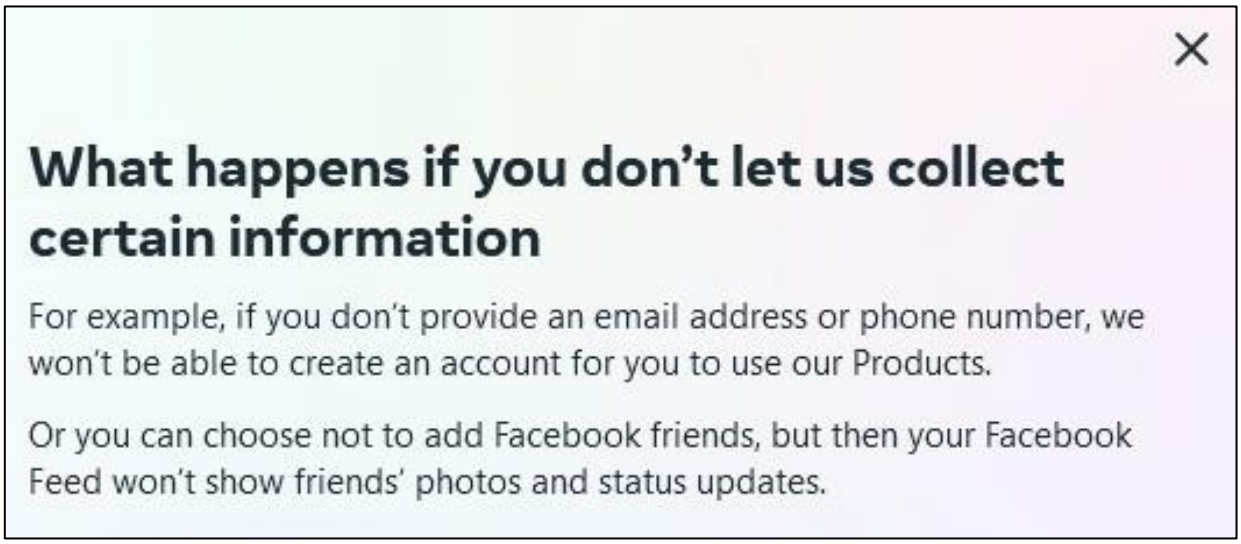
90. Although the Meta Data Policy makes general broad disclosures about the data it collects, the scope of Meta's "data license" is not unlimited. For example, by signing up for Meta, a Facebook user has not agreed to exchange with Meta the right for Meta to obtain their bank account information or Social Security number. Instead, the Meta Privacy Policy establishes a minimum amount of information users must provide directly to Meta to use Meta's products:



[17] *https://www.businessinsider.com/facebook-changes-free-and-always-will-be-slogan-on-home page-2019-8.*

[18] The hyperlink to Data Policy sends users to the Meta Privacy Policy at *https://www.facebook. com/privacy/policy/?entry point=data policy redirect&entry=0.*

91. When a Facebook user clicks the "Learn more" hyperlink to learn what "information is required" for Facebook to work, Meta provides examples of how choosing not to share information will prevent users from creating a Facebook account or using its features:



92. Meta's Terms of Service also expressly incorporates the Meta Privacy Policy by hyperlink, stating that "Our Privacy Policy explains how we collect and use your personal data to determine some of the ads you see and provide all of the other services described" in Meta's Terms of Service.

93. The Meta Privacy Policy has a section titled "What information do we collect?" in which Meta tells users:

> Meta, we use information to provide you with a more personal, secure, and meaningful experience. But where does that information come from? The information we collect comes from a variety of sources.... *And, sometimes businesses also share information with us like your activity on their websites. They may also share experiences you have offline, like signing up for a Rewards card with your email address.* This makes it easier for them to share promotions, product information, and other ads with you through our ads consistent with the choices that you make.

(Emphasis added). *Id.*

94. The Meta Privacy Policy does not say that Meta actively solicits Facebook users' healthcare providers, health insurers, pharmacies, prescription drug companies, and other covered entities under 45 C.F.R. § 160.103 to become Meta Partners using Meta's business services.

95. The Meta Privacy Policy does not say that, in exchange for use of its Products, Meta will collect health information from a Facebook user's healthcare providers, health insurers, pharmacies, prescription drug companies, or other covered entities under 45 C.F.R § 160.103 about the Facebook user, including their communications, actions, and status as patients with those health entities.

96. In addition to not obtaining specific consent, Meta affirmatively promises users that it requires "Partners" to have the right to share the users' data before providing it to Meta.

97. Before April 2018, Meta's contract did not require Partners to have the lawful right to share user data before doing so:

Before April 19, 2018

Information from websites and apps that use our Services.
We collect information when you visit or use third-party websites and apps that use our Services (like when they offer our Like button or Facebook Log In or use our measurement and advertising services). This includes information about the websites and apps you visit, your use of our Services on those websites and apps, as well as information the developer or publisher of the app or website provides to you or us.

Information from third-party partners.
We receive information about you and your activities on and off Facebook from third-party partners, such as information from a partner when we jointly offer services or from an advertiser about your experiences or interactions with them.

After April 19, 2018

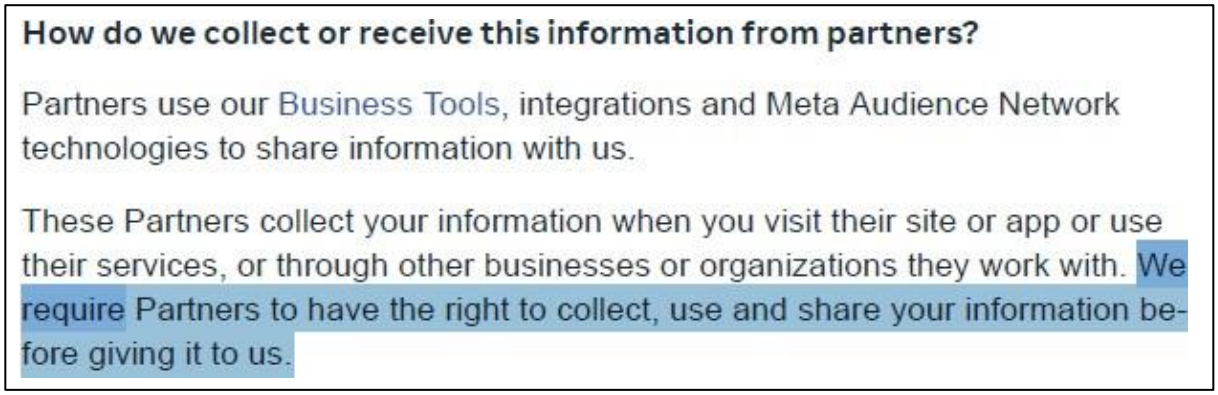
Information from partners.
Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third party data providers who have the rights to provide us with your information.

Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.

To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

98. Meta changed this provision again in July 2022 to remove the word "lawful" while still promising that it requires partners to have the right to share patient information with Meta:[19]

99. Meta does not verify that healthcare providers or covered entities have provided


How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

adequate notice and obtained valid consent or authorization to share their patients' data with Meta.[20]

100. Meta's contract with healthcare providers for use of the Meta Pixel does not mention HIPAA.

101. Meta does not use an advanced technical system to monitor whether Meta Collection Tools are installed on websites that will transmit individually-identifiable health information to Meta. To the contrary, Meta Health urges healthcare providers and other covered entities to use Meta Collection Tools to target ads to patients.

102. Meta maintains a "Health" marketing division called Meta Health, with a page at *https://www.facebook.com/business/industries/consumer-goods/healthcare* where Meta offers

[19] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), *https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartners Vendors.*

[20] The European Union recently ruled that Meta's attempt to obtain consent from users by including a clause in its terms and conditions allowing Meta to collect their data for personal advertising violated Europe's General Data Protection Regulation. Adam Satariano, *Meta's Ad Practices Ruled Illegal Under E.U. Law*, N.Y. Times (Jan. 4, 2023), *https://www.nytimes.com/2023/01/04/technology/meta-facebook-eu-gdpr.html.*

advertisers the chance to "get help growing your healthcare business" and explains how "Healthcare marketers are partnering with Meta."

103. The underlying metadata written for this page by Meta describe the page keywords to include: "<meta name="keywords" content="healthcare, marketers, Facebook, meta for business, healthcare business, virtual healthcare, preventative healthcare"/>."

104. Meta Health is dedicated to helping web developers and advertisers in healthcare related industries to increase their marketing spend with Meta and improve their marketing campaigns using Meta Collection Tools.

105. Meta Health's role is to "inform" healthcare marketers "to think about how we can really disrupt health and how we market to patients."[21]

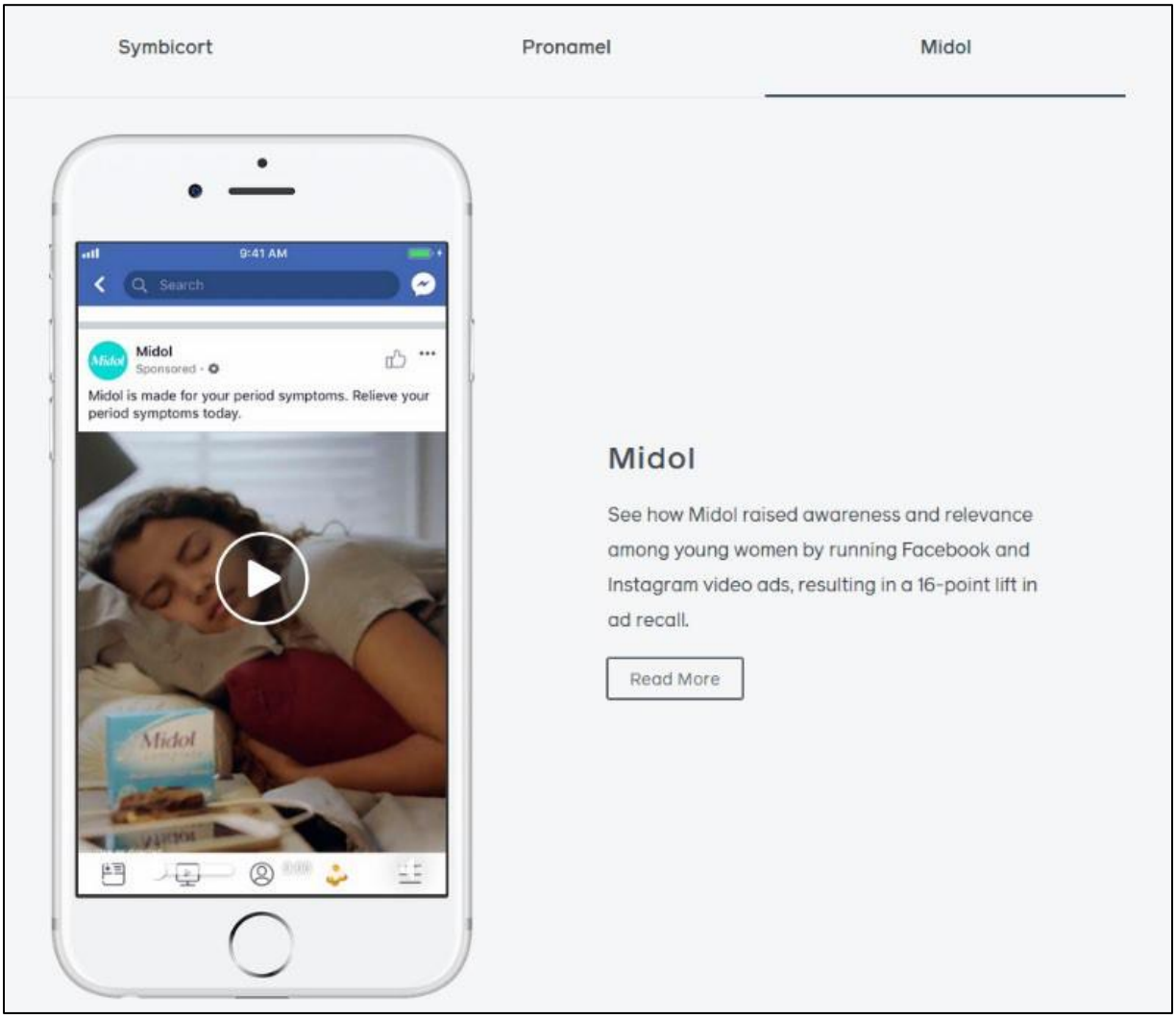
106. Meta Health employees are assigned to specific healthcare providers and other covered entities to encourage and aid their use of Meta Collection Tools for targeting patients.

107. Meta provides guidance and resources for web developers and advertisers on a dedicated webpage at *https://www.facebook.com/business/industries/health*. Among other things, this webpage includes examples of advertising campaigns so that web developers and advertisers can "See how health brands are reaching new audiences with Facebook advertising."

108. The underlying metadata written for this page by Meta describes the page keywords to include: ""<meta name="keywords" content="Facebook for health, Facebook marketing for health communities, Facebook ad solutions for health brands, social media marketing, Facebook video ads Facebook for mobile advertising, health campaign marketing, reach new patients online Facebook ads, advertising on Facebook"/>."

[21] Facebook Disrupting Health: A Conversation with Jasson Gilmore, *https://www.facebook.com/business/industries/health?deeplink=829704181304626*.

109. For example, Meta highlights an advertising campaign aimed at "young women" through video ads promising to "Relieve your period symptoms today." [22]



110. Meta has also engaged in similar advertising campaigns relating to treatments for acne, allergies, arthritis, birth control, diabetes, erectile dysfunction, hair loss, high cholesterol, migraines, and many more prescription drugs and treatments.[23]

[22] *Midol* (2023), *https://www.facebook.com/business/success/2-midol.*
[23] *See generally* Meta, Get winning advertising solutions from businesses like yours (2023), *https://www.facebook.com/business/success/categories/health-pharmaceuticals.* The "marketing case studies" on this page change on occasion.

DEFENDANT'S CONDUCT VIOLATES FEDERAL AND STATE PRIVACY LAWS

The HIPPA Privacy Rule Protects Patient *Healthcare* Information

111. Patient healthcare information in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

112. The HIPAA Privacy Rule, located at 45 C.F.R. § 160 and 45 C.F.R. § 164 (A) and (E): "establishes national standards to protect individuals' medical records and other individually-identifiable health information (collectively defined as 'protected health information') and applies to health plans, healthcare clearinghouses, and those healthcare providers that conduct certain healthcare transactions electronically.[24]

123. The Privacy Rule broadly defines "protected health information" ("PHI") as "individually-identifiable health information" ("IIHI") that is "transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

124. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of healthcare to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

[24] HHS.gov, *Health Information Privacy* (Mar. 31, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.*

125. Under the HIPAA de-identification rule, "health information is not individually-identifiable only if: (1) an expert "determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information" and "documents the methods and results of the analysis that justify such determination"; or (2) "the following identifiers of the individual or of relatives, employers, or household members of the individual are removed:

a. Names;

b. Medical record numbers;

c. Account numbers;

d. Device identifiers and serial numbers;

e. Web Universal Resource Locators (URLs);

f. Internet Protocol (IP) address numbers; … and

g. Any other unique identifying number, characteristic, or code…; and" the covered entity must not "have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is subject of the information." 45 C.F.R. § 164.514.

126. The HIPAA Privacy Rule requires any "covered entity"—which includes healthcare providers like Jefferson Health—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ 160.103, 164.502.

127. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually-identifiable health information relating to an individual." The statute states that a "person… shall be considered to

have obtained or disclosed individually-identifiable health information … if the information is maintained by a covered entity … and the individual obtained or disclosed such information without authorization." 42 U.S.C. § 1320(d)(6).

128. The criminal and civil penalties imposed by 42 U.S.C. § 1320(d)(6) apply directly to Meta when it is knowingly obtaining individually-identifiable health information relating to an individual, as those terms are defined under HIPAA.

129. Violation of 42 U.S.C. § 1320(d)(6) is subject to criminal penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320(d)(6)(b). In such cases, an entity that knowingly obtains individually-identifiable health information relating to an individual "shall be fined not more than $250,000, imprisoned not more than 10 years, or both." 42 U.S.C. § 1320(d)(6)(b)(1).

HIPAA Protects Patient *Status* Information

130. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.

131. Guidance from HHS confirms that HIPAA protects patient status:

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data.… **If such information was listed with health condition, healthcare provision or payment data, such as an indication that an individual was treated at a certain clinic, then this information would be PHI.**[25]

[25] Office for Civil Rights, *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (Nov. 26, 2012) (emphasis added); *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf.*

132. HHS' guidance for marketing communications states that healthcare providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. … Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. Moreover, **covered entities may not sell lists of patients to third parties without obtaining** authorization from each person on the list.[26]

133. HHS has previously instructed that the HIPAA privacy Rule protects patient status:

a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);

b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

[26] Office for Civil Rights, *Marketing* at 1-2 (Apr. 3, 2003), *https://www.hhs.gov/ sites/default/files /ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf* (emphasis added).

HIPAA's Protections Do Not Exclude Internet Marketing

134. In December 2022, HHS issued a bulletin "to highlight the obligations" of healthcare providers and their business associates under the HIPAA Privacy Rule "when using online tracking technologies" such as the "Meta Pixel," which "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[27]

135. In this bulletin, HHS confirmed that HIPAA applies to healthcare providers' use of tracking technologies like the Meta Pixel.[28] Among other things, HHS explained that healthcare providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address) even if no treatment information is included and even if the individual does not have a relationship with the healthcare provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually-identifiable health information (IIHI) that the individual providers when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of healthcare services. **This is because, when a regulated entity collects the individual's IIHI**

[27] HHS.gov, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information* (Dec. 1, 2022), *https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html.*

[28] HHS.gov, *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates* (Dec. 1, 2022), *https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.*

> **through its website or mobile app, the information connects the individual to the regulated entity (*i.e.* it is indicative that the individual has received or will receive healthcare services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or healthcare or payment for care**.

136. HHS explained that tracking technologies on healthcare providers' patient portals "generally have access to PHI" and may access diagnosis and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticate webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. **Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal**. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to **only** use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.

137. HIPAA applies to healthcare providers' webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> [T]racking technologies on unauthenticated webpages may access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a

> separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal … **[and pages] that address[] specific symptoms or health conditions,** such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering **credentials may have access to PHI in certain circumstances**. For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a healthcare provider. In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

138. As a result, a healthcare provider may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its website users and entered into a business associate agreement with the vendor:

> Regulated entities may identify the use of tracking technologies in their website or mobile app's privacy policy, notice, or terms and conditions of use. However, the Privacy Rule does **not** permit disclosures of PHI to a tracking technology vendor based solely on a regulated entity informing individuals in its privacy policy, notice, or terms and conditions of use that it plans to make such disclosures. Regulated entities must ensure that all tracking technology vendors have signed a BAA and that there is an applicable permission prior to a disclosure of PHI. If there is not an applicable Privacy Rule permission or if the vendor is not a business associate of the regulated entity, then the individual's HIPAA-compliant authorizations are required **before** the PHI is disclosed to the vendor. Website banners that ask users to accept or reject a website's use of tracking technologies, such as cookies, do **not** constitute a valid HIPAA authorization. [I]t is insufficient for a tracking technology vendor to agree to remove PHI from the information it receives or de-identify the PHI before the vendor saves the information. Any disclosure of PHI to the vendor without individuals' authorizations requires the vendor to have a signed BAA in place **and** requires that there is an applicable Privacy Rule permission for disclosure.

139. HHS's bulletin did not create any new obligations. Instead, it merely highlighted long-standing obligations based on previous guidance and rules that have been in place for decades.

The FTC Act Protects Health Information

140. In the context of this case, the FTC has made clear that "health information" is "anything that conveys information—or enables an information—about a consumer's health" and provides an example that location-data alone (such as repeated trips to a cancer treatment facility") "may convey highly sensitive information about a consumer's health." Jillson, Elisa, *Protecting the privacy of health information: A baker's dozen takeaways from FTC cases*, Federal Trade Commission (July 25, 2023), *https://www.ftc.gov/business-guidance/blog/2023/07/protecting-privacy-health-information-bakers-dozen-takeaways-ftc-cases*. The FTC has joined HHS in notifying HIPAA-covered entities and non-HIPAA-covered entities that sharing such "health information" with Google and Facebook is an unfair business practice under federal law:

> When consumers visit a hospital's website or seek telehealth services, they should not have to worry that their most private and sensitive health information may be disclosed to advertisers and other unnamed, hidden third parties," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The FTC is again serving notice that companies need to exercise extreme caution when using online tracking technologies and that we will continue doing everything in our powers to protect consumers' health information from potential misuse and exploitation."[29]

Pennsylvania Law Protects Health Information

141. For example, 28 Pa. Code § 115.27 provides that: all medical records and information: "shall be treated as confidential. Only authorized personnel shall have access to the records. The written authorization of the patient shall be presented and then maintained in the original record as authority for release of medical information outside the hospital."

[29] *FTC and HHS Warn Hospital Systems and Telehealth Providers About Privacy and Security Risks from Online Tracking Technologies*, Federal Trade Commission (July 20, 2023), *https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking*.

142. Thus, Pennsylvania law requires all hospitals, including Jefferson Health, to maintain all medical records and information within their control as confidential, rendering Jefferson Health's actions with respect to the interception and disclosure of its patients' health communications to Meta unlawful under Pennsylvania law.

Patients Have Protectable Property Interests
In Their Individually-Identifiable Health Information

143. Property is the right of any person to possess, use, enjoy, or dispose of a thing, including intangible things like data and communications. Plaintiffs and the Class members have a vested property right in their individually-identifiable health information.

144. Courts have described the concept of "property" broadly:

a. "property," as used in the Constitution, is a word of most general import and extends to every species of right and interest, capable of being enjoyed as such, upon which it is practicable to place a money value, *see Council Rock Sch. Dist. v. Land in Northampton Tp.*, 46 Pa. D. & C.2d 245, 248–49 (Pa. Com. Pl. 1968), *quoting* 26 Am. Jur. 2d, Eminent Domain, §173, p. 848 (1966);

b. *The Chesapeake and Ohio Ry. Co. v. Burkentine*, 45 Pa. D. & C.3d 344, 347 (Pa. Com. Pl. 1987) (describing property as "everything that has exchangeable value");

c. Also included in the bundle of rights constituting "property" is the right to exclude other persons from using the thing in question, *see Pet. of Borough of Boyertown*, 466 A.2d 239, 245 (Pa. Cmmw. 1983), *citing Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419 (1982).

145. Federal and state law grant patients the right to protect the confidentiality of data that identifies them as patients of a particular healthcare provider and restrict the use of their health data, including their status as a patient, to only uses related to their care or otherwise authorized by federal or state law in the absence of patient authorization.

146. A patient's right to protect the confidentiality of their health data and restrict access to this data is valuable.

147. In addition, patients enjoy property rights in the privacy of their health communications under statutes such as HIPAA; and 28 Pa. Code § 115.27. State health privacy laws and American courts have long recognized common law property rights in the content of a person's communications that are not to be used or disclosed to others without authorization.

148. Property rights in communications and information privacy are established by:

a. The Electronic Communications Privacy Act, including Title I (the Wiretap Act); Title II (the Stored Communications Act); and Title III (the Pen Register Act);

b. State laws, including 28 Pa. Code § 115.27; and

c. Common law information property rights regarding the exclusive use of confidential information that have existed for centuries and continue to exist, s*ee Folsom v. Marsh*, 9 F. Cas. 342, 346 (C.C.D. Mass. 1841) (Story, J); *Baker v. Libbie*, 210 Mass. 599, 602 (1912); *Denis v. LeClerc*, 1 Mart. (La.) 297 (1811).

149. Meta's CEO Mark Zuckerberg has expressly acknowledged that Meta users have an ownership interest in their data. In 2010, when Meta first revealed its "Download Your Information" tool, Zuckerberg stated that, "People own and have control over all info they put into Facebook and 'Download Your Information' enables people to take stuff with them."[30] Although Zuckerberg's statements regarding people's ability to "control" the information "put into Facebook" and the ability to access all such data via DYI is not true, his statement about data ownership is true.

150. Jefferson Health's unauthorized interception and disclosure of Plaintiffs' and the Class members' individually identifiable health information violated their property rights to control

[30] *https://techcrunch.com/2010/10/06/facebook-now-allows-you-to-download-your-information/.*

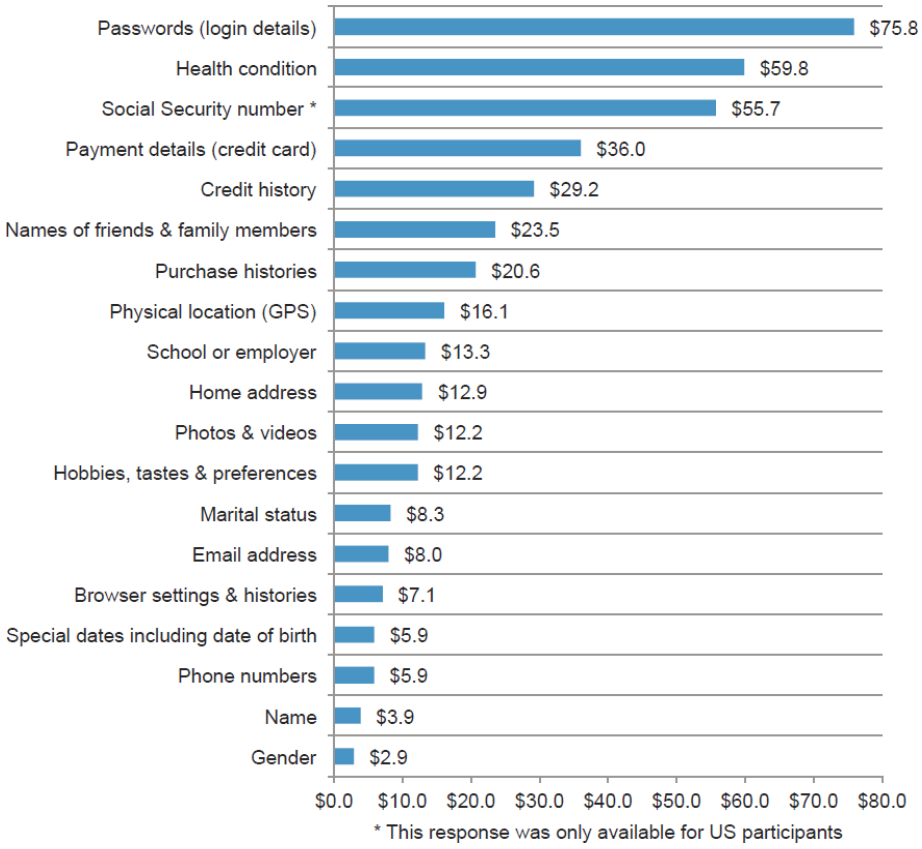
how their data and communications are used and who may be the beneficiaries of their data and communications.

The Information Jefferson Health Intercepts And Discloses To Meta Without Plaintiffs' Or The Class Members' Consent Has Actual, Measurable Monetary Value

151. Meta "generate[s] substantially all of [its] revenue from advertising."[31]

152. Meta annually receives billions of dollars of unearned advertising sales revenue from Meta healthcare Partners, including Jefferson Health, who are targeting Facebook users based on their health information.

153. The data that Meta collects without authorization has monetary value. For example, a 2015 study found respondents placed a value of $59.80 on an individual's health information:



[31] Meta 2022 Annual Report at 17.

THE PARTIES

154. Jefferson Health is a multi-state non-profit health system based in Philadelphia, Pennsylvania that consists of Thomas Jefferson University Hospital, Jefferson Hospital for Neuroscience, Methodist Hospital, Jefferson at the Navy Yard, and Jefferson-Voorhees. Jefferson Health encourages its patients, which number in the thousands, to use and communicate with their medical providers through Jefferson Health's web properties.

155. Nancy Murphy is an adult person who resides in the Commonwealth of Pennsylvania. Ms. Murphy opened a Facebook account before 2018 and has continuously maintained this account to the present. Ms. Murphy has been a patient of Jefferson Health since before 2018. Before 2018, Ms. Murphy created an account on Jefferson Health's web properties by entering her name, mailing address, date of birth, gender, phone number, e-mail address and abbreviated Social Security number, and answering questions from a third-party verification system.

156. During the relevant period, Ms. Murphy sought treatment from Katie Dougherty, D.O. (family medicine) and the Cardiology/Pulmonology, Diabetes (obesity, high blood pressure, heart disease), Family Medicine, Gynecology, Hematology, Internal Medicine, and Sleep Disorder Departments at Thomas Jefferson University Hospital, among others. Ms. Murphy received medical treatments for anemia, asthma, diabetes management, gastrointestinal issues, gynecological issues, hypertension/heart health, mammograms, obesity/weight management, dermatology/skin issues, and sleep apnea, among others.

157. When Meta Collection Tools were present, at the same time she was seeking diagnosis and treatment for these conditions, Ms. Murphy used the MyJeffersonHealth website (located at *https://www.jeffersonhealth.org/home*) and the MyChart patient portal (located at

https:// jeffersonhealthcare.org/mychart/), to search for medical providers, schedule appointments with these providers, communicate with these providers, view test results, read doctors' notes and care recommendations, review prescription and treatment information related to her specific symptoms, diagnoses, treatments, and medications, and request prescription refills.

158. When Ms. Murphy engaged in these communications with Jefferson Health's web properties, Meta's Collection Tools intercepted individually-identifiable patient information and patient health information that included: her status as a Jefferson Health patient, the dates and times she logged-in to the MyChart patient portal, and the webpages she clicked and viewed related to her medical providers, conditions, and treatments. Because Jefferson Health's and Meta's conduct was surreptitious and conducted through back-end electronic systems and processes, Plaintiffs will seek specific information about these intercepted and transmitted communications in discovery. However, at a minimum, when Ms. Murphy used her computer to log-in to the Jefferson Health MyChart patient portal, which she did many times during the relevant period in connection with communications about her medical providers, appointments, test results, treatments, and prescriptions, the Meta Pixel and Collection Tools on Jefferson Health's web properties sent at least the following personally identifiable patient information and patient health information to Meta:

a. Ms. Murphy was communicating with Jefferson Health on its *www.jefferson health.org* website;

b. Ms. Murphy engaged in an "ev" or "event," called a SubscribedButtonClick, or something substantially similar;

c. Descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

d. The content of the button Ms. Murphy clicked was "Login to myjeffersonhealth," or something substantially similar;

e. The page on which Ms. Murphy clicked the button was "Patient Portal," "Home," or something substantially similar;

f. Ms. Murphy had previously visited a Jefferson Health page;

g. Ms. Murphy's Internet Protocol address;

h. Identifiers that Facebook uses to identify Ms. Murphy and her device, including the c-user, datr, fr, and _fbp cookies; and

i. Browser attribute information sufficient to fingerprint Ms. Murphy's device.

159. As a result, the Meta Pixel and Collection Tools on Jefferson Health's web properties intercepted and disclosed to Meta information about Ms. Murphy's identity, her log-in to the patient portal, the and the content of the communications she made on Jefferson Health's web properties.

160. Jefferson Health never notified Ms. Murphy that either it or Meta would put individually-identifiable patient health information about her past, present, or future health conditions to their own commercial uses. Ms. Murphy never provided informed consent or written permission allowing Jefferson Health to send individually-identifiable patient health information about her past, present, or future health conditions to Meta. Ms. Murphy never provided informed consent or written permission allowing Jefferson Health or Meta to put individually-identifiable patient health information about her past, present, or future health conditions to their own commercial use.

161. Meta used the intercepted content of Ms. Murphy's communication with Jefferson Health to repeatedly serve her ads for the following prescription drugs "focused" on her status as a patient of Jefferson Health, the specific conditions for which she was being treated, the specific medications she was being prescribed, and symptoms related to those conditions, including:

a. Ozempic (type 2 Diabetes treatment); and

b. Mounjaro (type 2 Diabetes treatment).

162. Ms. Murphy routinely viewed these ads shortly after using Jefferson Health's web properties to schedule office visits, view her prescriptions, request prescription refills, or view webpages related to relevant conditions and treatments.

163. Robert Stewart is an adult person who resides in the Commonwealth of Pennsylvania. Mr. Stewart opened a Facebook account before 2018 and has continuously maintained this account to the present. Mr. Stewart has been a patient of Jefferson Health since before 2018. Before 2018, Mr. Stewart created an account on Jefferson Health's web properties by entering his name, mailing address, date of birth, gender, phone number, e-mail address and abbreviated Social Security number, and answering questions from a third-party verification system.

164. During the relevant period, Mr. Stewart sought treatment from Jefferson Abington Hospital, Jefferson Torresdale Hospital, Jefferson Health – Bala Cynwyd, and Urological Associates PC, Keino Johnson, D.O. (family medicine and internal medicine), and Marc Lavine, M.D. (urology) for multiple medical issues, including: diabetes (obesity, high blood pressure, heart disease), kidney stones (urology, cystoscopy), prostate health/screening, nicotine dependence/smoking cessation, Hepatitis C screening, and vaccines. When Meta Collection Tools were present, at the same time he was seeking diagnosis and treatment for these conditions, Mr. Stewart used the MyJeffersonHealth website (located at *https://www.jeffersonhealth.org/home*) and the MyChart patient portal (located at *https://jeffersonhealthcare.org/mychart/*), to search for medical providers, schedule appointments with these providers, view medical test results, read doctors' notes and care recommendations, and review prescription and treatment information related to his specific symptoms, diagnoses, treatments, and medications

165. When Mr. Stewart engaged in these communications with Jefferson Health's web properties, Meta's Collection Tools intercepted individually-identifiable patient information or patient health information that included his status as a Jefferson Health patient, the dates and times he logged-in to the MyChart patient portal, and the webpages he clicked and viewed related to his medical providers, conditions, and treatments. Because Jefferson Health's and Meta's conduct was surreptitious and conducted through back-end electronic systems and processes, Plaintiffs will seek specific information about these intercepted and transmitted communications in discovery. However, at a minimum, when Mr. Stewart used his computer to log-in to the Jefferson Health MyChart patient portal, which he did many times during the relevant period in connection with his search for medical providers, appointments, test results, treatments, and prescriptions, the Meta Pixel and Collection Tools on Jefferson Health's web properties sent at least the following personally-identifiable patient information and patient health information to Meta:

a. Mr. Stewart was communicating with Jefferson Health on its *www.jefferson health.org* website;

b. Mr. Stewart engaged in an "ev" or "event," called a SubscribedButtonClick;

c. Descriptive URLs that describe the categories of the website, categories that describe the current section of the website, and the referrer URL that caused navigation to the current page;

d. The content of the button Mr. Stewart clicked was "Login to myjeffersonhealth," or something substantially similar;

e. The page on which Mr. Stewart clicked the button was "Patient Portal," "Home," or something substantially similar;

f. Mr. Stewart had previously visited a Jefferson Health page;

g. Mr. Stewart's Internet Protocol address;

h. Identifiers that Facebook uses to identify Mr. Stewart and his device, including the c- user, datr, fr, and _fbp cookies; and

i. Browser attribute information sufficient to fingerprint Mr. Stewart's device.

166. As a result, the Meta Pixel and Collection Tools on Jefferson Health's web properties intercepted and disclosed to Meta information about Mr. Stewart's identity, his log-in to the patient portal, and the content of the communications he made on Jefferson Health's web properties.

167. Jefferson Health never notified Mr. Stewart that either it or Meta would put individually-identifiable patient health information about his past, present, or future health conditions to their own commercial uses. Mr. Stewart never provided informed consent or written permission allowing Jefferson Health send individually-identifiable patient health information about his past, present, or future health conditions to Meta. Mr. Stewart never provided informed consent or written permission allowing Jefferson Health or Meta to put individually-identifiable patient health information about his past, present, or future health conditions to their own commercial uses.

168. Meta used the intercepted content of Mr. Stewart's communication with Jefferson Health to serve him countless ads for the following prescription and over-the-counter drugs, products, and services "focused" on his status as a patient of Jefferson Health, the specific conditions for which he was being treated, and symptoms related to those conditions, including:

a. Ozempic (type 2 Diabetes treatment);

b. Metformin (type 2 Diabetes treatment);

c. Jardiance (type 2 Diabetes treatment);

d. Tzield (diabetes progression inhibitor);

e. BlueChew (erectile dysfunction treatment); and

f. EatingWell.com (weight-loss system).

169. Mr. Stewart routinely viewed these ads shortly after using Jefferson Health's web properties to schedule office visits, view his prescriptions, request prescription refills, or view webpages related to relevant conditions and treatments.

170. Meta maintains a history of every ad it has shown to Plaintiffs and the Class members, both on and off Meta's social media sites, including on Meta properties and the Facebook Audience Network through which Meta serves ads to Facebook users on non-Meta websites. Plaintiffs intend to seek this information in discovery to fully inform the scope of their claims and damages.

CLASS ACTION ALLEGATIONS

171. Plaintiffs bring this action as a class action under Federal Rules of Civil Procedure 23(a) and (b)(3) for:

> All persons whose protected health information was disclosed to Meta without authorization or consent through the Meta Collection Tools on Jefferson Health's web properties.

("the Class members").

172. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(1), because the Class members are so numerous and geographically dispersed that their joinder would be impracticable. Plaintiffs believe that Defendant's and Meta's business records will permit the identification of thousands of people meeting the Class definition.

173. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(2), because there are many common questions of facts and law concerning and affecting the Class members, including:

a. Whether Jefferson Health had a duty to protect and refrain from disclosing the Class members' individually-identifiable health information;

b. Whether Jefferson Health intentionally disclosed the Class members' individually-identifiable health information to Meta;

c. Whether the Class members consented to Jefferson Health's disclosure of their individually-identifiable health information to Meta;

d. Whether the Class members are entitled to damages because of Jefferson Health's conduct; and

e. Whether Jefferson Health's knowing disclosure of its patients' individually-identifiable health information to Meta is "criminal or tortious" under 18 U.S.C. § 2511(2)(d).

174. Plaintiffs also anticipate that Defendant will raise defenses common to the Class.

175. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(3), because Plaintiffs' claims are typical of the claims belonging to the Class members. Plaintiffs and the Class members were harmed by the same wrongful conduct perpetrated by Defendant that caused their individually-identifiable health information to be intercepted and disclosed without notice or consent. As a result, Plaintiffs' claims are based on the same facts and legal theories as the Class members' claims.

176. This action is properly maintained as a class action under Fed. R. Civ. P. 23(a)(4), because Plaintiffs will fairly and adequately protect the interests of all the Class members, there are no known conflicts of interest between Plaintiffs and the Class members, and Plaintiffs have retained counsel experienced in the prosecution of complex litigation.

177. Class certification is appropriate under Fed. R. Civ. P. 23(b)(3), because common questions of law and fact predominate over questions affecting the individual Class members, because a class action is superior to other available methods for the fair and efficient adjudication

of these claims and because important public interests will be served by addressing the matter as a class action. Further, the prosecution of separate actions by the individual Class members would create a risk of inconsistent and varying adjudications, establish incompatible standards of conduct for Defendant and substantially impair the Class members' ability to protect their interests.

TOLLING

178. Any statute of limitations applicable to Plaintiffs' claims has been tolled by Jefferson Health's actual knowledge and active, intentional efforts to conceal the actions, misrepresentations, and omissions alleged herein. Through no fault or lack of diligence, Plaintiffs and the Class members had no obvious way to discover Jefferson Health's deception and unlawful conduct.

179. Plaintiffs and the Class members did not discover and did not know of any facts that would have caused a reasonable person to suspect that Jefferson Health was acting unlawfully. Jefferson Health's alleged representations were material to Plaintiffs and the Class members at all relevant times. During any applicable statute of limitations, Plaintiffs and the Class members could not have discovered Jefferson Health's alleged wrongful conduct through the exercise of reasonable diligence.

180. At all relevant times, Jefferson Health was – and still is – under a continuous duty to disclose to Plaintiffs and the Class members the true nature of the disclosures being made and the lack of an actual "requirement" before it shared Plaintiffs' and the Class members' data with Meta.

181. Jefferson Health's knowingly, actively, affirmatively, or negligently concealed the facts alleged herein. Plaintiffs and the Class members reasonably relied on Jefferson Health's concealment.

182. For these reasons, all applicable statutes of limitation have been tolled based on the discovery rule and Jefferson Health's concealment, and Jefferson Health is estopped from relying on any statutes of limitations in defense of this action.

COUNT I
Violation of the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*

183. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

184. The Electronic Communications Privacy Act ("ECPA") prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

185. The ECPA protects both the sending and receipt of communications.

186. The ECPA provides a private right of action to any person whose electronic communications are intercepted. 18 U.S.C. § 2520(a).

187. Jefferson Health intentionally intercepted electronic communications that Plaintiffs and the Class members exchanged with Jefferson Health through the Meta Collection Tools installed on the Jefferson Health's web properties.

188. The transmissions of data between Plaintiffs and the Class members and Jefferson Health qualify as communications under the ECPA. 18 U.S.C. § 2510(12).

189. Jefferson Health contemporaneously intercepted and transmitted Plaintiffs' and the Class members' communications to Meta.

190. The intercepted communications include:

a. the content of Plaintiffs' and the Class members' registrations for patient portals, including clicks on buttons to "Register" or "Signup" for portals;

b. the content Plaintiffs' and the Class members' log in and log out of patient portals, including clicks to "Sign-in," "Log-in," "Sign-out," or "Log-out;"

c. the content of communications that Plaintiffs and the Class members exchange inside patient portals immediately before logging out of the portals;

d. the content of Plaintiffs' and the Class members' communications relating to appointments with medical providers;

e. the content of Plaintiffs' and the Class members' communications relating to specific healthcare providers, conditions, treatments, diagnoses, prognoses, prescription drugs, symptoms, insurance, and payment information; and

f. Full-string URLs that contain any information concerning the substance, purport, or meaning of patient communications with their health entities.

191. For example, Defendant's interception of the fact that a patient views a webpage like *https://www.jeffersonhealth.org/conditions-and-treatments/breast-cancer/treatments-we-offer* involves "content," because it communicates that patient's request for the information on that page.

192. The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. the cookies Jefferson Health and Meta use to track Plaintiffs' and the Class members' communications;

b. Plaintiffs' and the Class members' browsers;

c. Plaintiffs' and the Class members' computing devices;

d. Jefferson Health's web-servers or webpages where the Meta Collection Tools are present;

e. Meta's web-servers; and

f. the Meta Collection Tools source code Jefferson Health deploys on its web properties to acquire Plaintiffs' and the Class members' communications.

193. Meta is not a party to Plaintiffs' and the Class members' communications with Jefferson Health.

194. Jefferson Health transmits the content of Plaintiffs' and the Class members' communications to Meta through the surreptitious redirection of those communications from the Plaintiffs' and the Class members' computing devices.

195. Plaintiffs and the Class members did not consent to Meta's acquisition of their patient portal, appointment, and phone call communications with Jefferson Health.

196. Meta did not obtain legal authorization to obtain Plaintiffs' and the Class members' communications with Jefferson Health relating to communications with their health entities.

197. Meta did not require Jefferson Health to obtain the lawful rights to share the content of Plaintiffs' and the Class members' communications relating to patient portals, appointments, and phone calls.

198. Any purported consent that Meta received from Jefferson Health to obtain the content of Plaintiffs' and the Class members' communications was not valid.

199. In disclosing the content of Plaintiffs' and the Class members' communications relating to patient portals, treatments, conditions, and appointments, Jefferson Health had a purpose that was tortious, criminal, and designed to violate state constitutional and statutory provisions including:

a. the unauthorized disclosure of individually-identifiable health information is tortuous in and of itself regardless of whether the means deployed to disclose the information violates the Wiretap Act or any subsequent purpose or use for the acquisition. Jefferson Health intentionally committed a tortious act by disclosing individually-identifiable health information without authorization to do so.

b. the unauthorized acquisition of individually-identifiable health information is a criminal violation of 42 U.S.C. § 1320d-6 regardless of any subsequent purpose or use of the individually-identifiable health information. Jefferson Health intentionally violated 42 U.S.C. 1320d-6 by intentionally disclosing

individually-identifiable health information without authorization.

c. a violation of HIPAA, particularly 42 U.S.C. § 1320d-6, which is a criminal offensive punishable by fine or imprisonment with *increased penalties* where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage [or] personal gain." Jefferson Health intentionally violated the enhanced penalty provision of 42 U.S.C. § 1320d-6 by disclosing the individually-identifiable health information "with intent to sell transfer or use" it for "commercial advantage [or] personal gain."

d. a knowing intrusion upon Plaintiffs' and the Class members' seclusion;

e. trespass upon Plaintiffs' and the Class members' personal and private property via the placement of an _fbp cookie associated with Jefferson Health's web properties on Plaintiffs' and the Class members' personal computing devices;

f. the requirement under 28 Pa. Code § 115.27 that healthcare providers maintain the confidentiality of patient health records; and

g. violation of the federal wire fraud statutes at 18 U.S.C. §§ 1343 (fraud by wire, radio, or television) and 1349 (attempt and conspiracy), which prohibit a person from "devising or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate … commerce, any writing, signs, signals, pictures, or sounds for purpose of executing such scheme or artifice."

200. The federal wire fraud statute, 18 U.S.C. § 1343, has four elements: (1) that the defendant voluntarily and intentionally devised a scheme to defraud another out of money or property; (2) that the defendant did so with the intent to defraud; (3) that is was reasonably foreseeable that interstate wire communications would be used; and (4) that interstate wire communications were in fact used. The attempt version of the wire fraud statute provides that

"[a]ny person who attempts or conspires to commit any offense under this chapter shall be subject to the same penalties as those prescribed for the offense, the commission of which was the object of the attempt or conspiracy." 18 U.S.C. § 1349.

201. Jefferson Health's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policies set forth above, including the statements and omissions recited in the breach of contract and negligence claims below;

b. the placement of the _fbp cookie on patient computing devices disguised as a first-party cookie of Jefferson Health's web properties rather than a third-party cookie from Meta.

202. Jefferson Health acted with the intent to defraud in that it willfully invaded and took the Named Plaintiffs' and the Class members' property:

a. property rights to the confidentiality of their individually-identifiable health information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

203. Jefferson Health acted with the intent to defraud in that it willfully invaded and took the Named Plaintiffs' and the Class members' property:

a. with knowledge that (1) Jefferson Health did not have the right to share such data without written authorization; (2) courts had determined that a healthcare providers' use of the Meta Pixel gave rise to claims for invasion of privacy and violations of state criminal statutes; (3) a reasonable Facebook user would not understand that Meta was collecting their individually-identifiable health information based on their activities on Jefferson Health's web properties; (4) "a reasonable Facebook user would be shocked to realize" the extent of Meta's collection of individually-identifiable health information; (5) a Covered Incident had occurred which required a report to be made to the FTC pursuant to Meta's consent decrees with the FTC; and (6) the subsequent use of health information for advertising was a

further invasion of such property rights in making their own exclusive use of their individually-identifiable health information for any purpose not related to the provision of their healthcare; and

b. with the intent to (1) acquire Plaintiffs and the Class members' individually-identifiable health information without their authorization and without their healthcare providers or covered entities obtaining the right to share such information; (2) use the Named Plaintiffs' and the Class members' individually-identifiable health information without their authorization; and (3) gain access to the Named Plaintiffs' and the Class members' personal computing devices through the _fbp cookie disguised as a first-party cookie.

204. Any purported consent provided by Jefferson Health using the Meta Collection Tools had a purpose that was tortious, criminal, and in violation of state constitutional and statutory provisions because it constitutes:

a. knowing intrusion into a private matter that would be highly offensive to a reasonable person;

b. a violation of 42 U.S.C. § 1320d-6, which is a criminal offense punishable by fine or imprisonment and that includes increased penalties where "the offense is committed with intent to sell, transfer, or use individually-identifiable health information for commercial advantage [or] personal gain."

c. trespass;

d. breach of fiduciary duty; and

e. a violation of various state health privacy and computer privacy statutes, including the CCPA.

205. Plaintiffs and the Class members have suffered damages because of Jefferson Health's violations of the ECPA that include:

a. eroding the essential, confidential nature of the provider-patient relationship;

b. failing to provide Plaintiffs and the Class members with the full value of the medical services for which they paid, which

included a duty to maintain the confidentiality of their patient information;

c. deriving valuable benefits from using and sharing the contents of Plaintiffs' and the Class members' communications on its web properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. depriving Plaintiffs and the Class members of the value of their individually-identifiable health information;

e. diminishing the value of Plaintiffs' and the Class Members' property rights in their individually-identifiable health information; and

f. violating Plaintiffs' and the Class members' privacy rights by sharing their individually-identifiable health information for commercial use.

206. For Jefferson Health's violations set forth above, Plaintiffs and the Class members seek appropriate equitable or declaratory relief, including injunctive relief; actual damages and "any profits made by [Jefferson Health] as a result" of its violations or the appropriate statutory measure of damages; punitive damages in an amount to be determined by a jury; and a reasonable attorney's fee and other litigation costs reasonably incurred pursuant to 18 U.S.C § 2520.

207. Unless enjoined, Jefferson Health will continue to commit the violations of law alleged here.

208. Plaintiffs want to continue to communicate with their healthcare provider through online platforms but have no practical way of knowing if their communications are being intercepted and disclosed to Meta, and thus continue to be at risk of harm from Jefferson Health's conduct.

209. Pursuant to 18 U.S.C. § 2520, Plaintiffs and the Class members seek monetary damages for the *greater of* (i) the sum of the actual damages suffered by the plaintiff and any

profits made by Jefferson Health as a result of the violation or (ii) statutory damages of whichever is greater of $100 a day for each violation or $10,000.

COUNT II
Breach of Contract

210. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

211. Jefferson Health requires patients who use its website to agree to the "Terms and Conditions" to "access and use [the] site and any page contained [within]… *www.jefferson health.org*."[32]

212. The "Terms and Conditions" is a binding contract on Jefferson Health.

213. Jefferson Health's "Privacy Practices" are expressly incorporated into the Terms and Conditions.

214. Jefferson Health's "Terms and Conditions" for the MyJeffersonHealth patient portal also expressly incorporates Jefferson Health's "Privacy Practices."[33]

215. Jefferson Health's Privacy Practices makes express promises that:

a. Jefferson Health understands that information about you and your health is very personal. Therefore, we strive to protect your privacy. We are required by law to maintain the privacy of our patients' protected health information, *see* Jefferson Health Notice of Privacy Practices *https://www.jeffersonhealth.org/ privacy-practices*;

b. We will obtain your written permission when the uses and disclosures of PHI are for marketing purposes or other activities where we receive remuneration in exchange for disclosing such PHI, *id*.;

[32] *https://www.jeffersonhealth.org/terms-and-conditions.*

[33]*See htttps://mychart.jefferson.edu/mychart/Authentication/Login?mode=stdfile&option=terms andconditions*. ("Individual is responsible for viewing and abiding by the terms and conditions of use and the privacy statements on the other Web sites.").

> c. Should we wish to disclose your PHI in any manner that would constitute a sale of your PHI, we will obtain your written authorization to do so, *id*.; and
>
> d. You may visit our website without submitting any information about yourself. If you send us e-mail or subscribe to one of our on-line publications, you will be asked to submit information about yourself. We will use this information for replying to your message or forwarding the requested material. We do not share this information with any other partners, affiliates or members of JHS. Our website may log the IP addresses of visitors, but only to administer the site and diagnose problems with our server. IP addresses are not used to identify individuals, *id*.

216. Jefferson Health breached these contractual promises in many ways, including by:

> a. routinely sharing patient portal login information with Meta;
>
> b. disclosing patient identifiers including, IP addresses, device identifiers, and URLs; and
>
> c. disclosing the content of patient communications containing private health information to Meta for marketing purposes and commercial gain.

217. As a direct and proximate result of Jefferson Health's breaches of contract, Plaintiffs and the Class members did not receive the full benefit of the bargain of their contract with Jefferson Health in that Jefferson Health overcharged Plaintiffs and the Class members by collecting data in excess of the "data license" that was agreed upon in the contract between Plaintiffs and the Class members and Jefferson Health in the Jefferson Health Privacy Practices and Terms and Conditions. Specifically, as set forth above, Jefferson Health expressly promised that its "data license" would not include the divulgence or sale of Plaintiffs' and the Class members' confidential health information.

218. Plaintiffs and the Class Members suffered damages because of Jefferson Health's breaches of contract that include:

a. suffering actual, nominal monetary damages measured by the loss in value of the medical services provided, and the loss in value of Plaintiffs' and the Class members' protected health information;

b. failing to provide Plaintiffs and the Class members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;

c. deriving valuable benefits from using and sharing the contents of Plaintiffs' and the Class members' communications on its web properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. depriving Plaintiffs and the Class members of the value of their individually-identifiable health information;

e. diminishing the value of Plaintiffs' and the Class Members' property rights in their individually-identifiable health information; and

f. depriving Plaintiffs and the Class members of part of the benefit of the bargain from their agreement to receive medical services from Jefferson Health because the data license for Defendant's services does not authorize it to share or use their individually-identifiable health information for commercial purposes.

COUNT III
Negligence

219. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

220. Plaintiffs and the Class members have communicated individually-identifiable patient health information to Jefferson Health through its web properties, *https://www.jefferson health.org/home*, the MyJeffersonHealth online portal, and the MyJeffersonHealth Mobile Application and/or received healthcare services from doctors employed by Jefferson Health.

221. By virtue of creating and maintaining its web properties as a public healthcare resource and its employment relationship with its doctors, Jefferson Health has assumed a duty to

keep confidential all individually-identifiable patient health information Plaintiffs and the Class members communicate.

222. Jefferson Health assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable patient health information confidential by issuing Patient Rights & Responsibilities representing that patient: "have the right to… discuss your care in places designed to protect your privacy… [and] [e]xpect all communications and records related to care, including who is paying for your care, to be treated as private." *See* Jefferson Health Patient Rights & Responsibilities, *https://www.jeffersonhealth.org/your-health/patients-guests/patient-rights-responsibilities/patient-rights-statement*.

223. Jefferson Health assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable patient health information confidential by issuing a Notice of Privacy Practices that represents: "Jefferson Health understands that information about you and your health is very personal. Therefore, we strive to protect your privacy. We are required by law to maintain the privacy of our patients' protected health information." *See* Jefferson Health Notice of Privacy Practices *https://www.jeffersonhealth.org/privacy-practices*.

224. Jefferson Health assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable patient health information confidential by issuing a Notice of Privacy Practices representing that: "We will obtain your written permission when the uses and disclosures of PHI are for marketing purposes or other activities where we receive remuneration in exchange for disclosing such PHI." *Id*.

225. Jefferson Health assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable patient health information confidential by issuing a Notice of Privacy

Practices representing that: "Should we wish to disclose your PHI in any manner that would constitute a sale of your PHI, we will obtain your written authorization to do so." *Id*.

226. Jefferson Health assumed a duty to keep Plaintiffs' and the Class members' individually-identifiable patient health information confidential by issuing an Online Privacy Statement representing that:

> *You may visit our website without submitting any information about yourself.* If you send us e-mail or subscribe to one of our on-line publications, you will be asked to submit information about yourself. We will use this information for replying to your message or forwarding the requested material. *We do not share this information with any other partners, affiliates or members of JHS. Our website may log the IP addresses of visitors, but only to administer the site and diagnose problems with our server. IP addresses are not used to identify individuals*.

See Jefferson Health Online Privacy Statement, *https://www.jeffersonhealth.org/privacy-practices /online-privacy-statement*.

227. Jefferson Health has a legal duty not to disclose Plaintiffs' and the Class members' medical records for marketing purposes without their express written authorization under multiple federal laws. See, e.g., 42 U.S.C. § 1320; 45 C.F.R. §§ 164.501; 164.508(a)(3), 164.514(b)(2)(i).

228. Jefferson Health has a legal duty to keep Plaintiffs' and the Class members' medical records confidential and private absent express written authorization under Pennsylvania law. *See, e.g.*, 28 Pa. Code § 115.27.

229. Jefferson Health has breached the various duties of care it owes and assumed by placing computer code on its web properties that intercepts the characteristics and content of communications about individually-identifiable patient health information and automatically transmits this data to Meta, putting this data to its own commercial use, and allowing Meta to put

this data to its own commercial use, without providing adequate notice to users of its web properties, or receiving their informed consent.

230. Plaintiffs and the Class members have suffered damages because of Jefferson Health's breach of its various duties of care that include:

a. eroding the essential, confidential nature of the provider-patient relationship;

b. failing to provide Plaintiffs and the Class members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;

c. deriving valuable benefits from using and sharing the contents of Plaintiffs' and the Class members' communications on its web properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. depriving Plaintiffs and the Class members of the value of their individually-identifiable health information;

e. diminishing the value of Plaintiffs' and the Class Members' property rights in their individually-identifiable health information; and

f. violating Plaintiffs' and the Class members' privacy rights by sharing their individually-identifiable health information for commercial use.

231. By sharing Plaintiffs' and the Class members' individually-identifiable patient health information with Meta in contravention of many duties requiring it to keep such information private, putting this information to its own commercial use without notice or consent, and allowing Meta to put this information to commercial use without notice or consent, Jefferson Health proximately caused the damages claimed herein.

COUNT IV

Invasion of Privacy - Intrusion Upon Seclusion

232. Plaintiffs incorporate the foregoing allegations as if fully set forth herein.

233. By collecting and disseminating the content of Plaintiffs' and the Class members' communications without their knowledge, Jefferson Health intentionally intruded into a realm in which Plaintiffs and the Class members have a reasonable expectation of privacy.

234. The communications at issue regarding the Named Plaintiffs include patient portal logins and communications regarding doctors, conditions, treatments, symptoms, payments, and other health-related communications content.

235. Plaintiffs and the Class members enjoyed objectively reasonable expectations of privacy in their communications with Jefferson Health relating to the respective patient portals, appointments, and health information and communications based on

a. Jefferson Health's status as their healthcare provider and the reasonable expectations of privacy that attach to patient-provider relationships;

b. HIPAA;

c. the ECPA;

d. Meta's promise that it would "require" Partners to have the right to share their data before Meta would collect it; and

e. Pennsylvania medical privacy laws.

236. Furthermore, Plaintiffs and the Class members maintained a reasonable expectation of privacy when providing their patient medical data to Jefferson Health and when communicating through Jefferson Health's web properties.

237. Patient medical data is widely recognized by society as sensitive information that cannot be shared with third parties without the patients' consent.

238. For example, public polling shows that, "[n]inety-seven percent of Americans believe that doctors, hospitals, labs and health technology systems should not be allowed to share or sell their sensitive health information without consent."[34]

239. Jefferson Health provided Meta with unwanted access to Plaintiffs' and the Class members' data, including but not limited to their patient status, the dates and times Plaintiffs and the Class members logged in or out of patient portals, and the communications Plaintiffs and the Class members exchanged while logged in to patient portals.

240. Jefferson Health's intrusion was also accomplished by placing the _fbp cookie on the Plaintiffs' and the Class members' computing devices through its own web-servers.

241. By deploying and disguising the third-party _fbp cookie as a first-party cookie from Jefferson Health, Defendant ensured that Meta could hack its way around attempts Plaintiffs and the Class members might make to prevent Meta's tracking with cookie blockers.

242. In designing the _fbp cookie as a disguised first-party cookie, Jefferson Health was aware that, like other websites that include sections where users' sign in to an account, Jefferson Health's web properties would require first-party cookies to be enabled for a patient to access the patient portal or other username / password protected "secure" part of the its web properties.

243. With first-party cookies being required for use of a patient portal and the Meta _fbp cookie disguised as a first-party cookie, Jefferson Health was able to implant its tracking device on the computing devices of the Named Plaintiffs and the Class members even where Plaintiffs or Class members made attempts to stop third-party tracking with cookie blockers.

[34] *Poll: Huge majorities wants control over health info,* Healthcare Finance (Nov. 10, 2020), https://www.healthcarefinancenews.com/news/poll-huge-majorities-want-control-over-health-info.

244. Jefferson Health's deployment of the _fbp cookie as a third-party cookie disguised as a first party cookie that is placed on Plaintiffs and the Class members' computing devices is a highly offensive intrusion upon seclusion regardless of whether any information was further re-directed from the Plaintiffs or Class members computing devices to Meta.

245. Jefferson Health's intrusion into Plaintiffs' and the Class members' privacy, including the placement of the _fbp tracking cookie on Plaintiffs' and the Class members' devices, would be highly offensive to a reasonable person, namely because it occurred without Plaintiffs' and the Class members' consent or knowledge and violated HIPAA, the CCPA, the ECPA, the FTC Act, and Class members' property rights.

246. Placement of the _fbp cookie was highly offensive to a reasonable person because:

a. It involved placement of a tracking tool on Plaintiffs' and the Class members' personal communications and computing devices while they were exchanging communications in what should have been a private conversation with their healthcare provider – and that tracking tool persisted on patient devices; and

b. Jefferson Health designed the _fbp tracking tool so that a patient could not securely login to the patient portal without Meta being able to download its tracking tool onto the Plaintiffs' and the Class members' communications devices.

247. Plaintiffs and the Class members have suffered damages because of Jefferson Health's intrusion upon seclusion, that include:

a. eroding the essential confidential nature of the provider-patient relationship;

b. failing to provide Plaintiffs and the Class members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of their patient information;

c. deriving valuable benefits from using and sharing the contents of Plaintiffs' and the Class members' communications on its

web properties without their knowledge or informed consent, and without providing any compensation for the information it used or shared;

d. depriving Plaintiffs and the Class members of the value of their individually-identifiable health information;

e. diminishing the value of Plaintiffs' and the Class Members' property rights in their individually-identifiable health information; and

f. violating Plaintiffs' and the Class members' privacy rights by sharing their individually-identifiable health information for commercial use.

248. Jefferson Health's intrusion into Plaintiffs' and the Class members' seclusion was with oppression, fraud, or malice.

COUNT V
Unjust Enrichment

249. Plaintiffs reallege and incorporate by reference each allegation in the preceding and succeeding paragraphs.

250. Jefferson Health has wrongfully and unlawfully transmitted, received, used, and sold Plaintiffs' and the Class members' individually-identifiable health information without their consent for substantial profits.

251. Plaintiffs' and the Class members' individually-identifiable health information conferred an economic benefit on Jefferson Health.

252. Jefferson Health has been unjustly enriched at the expense of the Plaintiffs and the Class members.

253. Jefferson Health has unjustly retained the benefits of its unlawful and wrongful conduct.

254. It would be inequitable and unjust for Jefferson Health to retain any of the unlawful proceeds resulting from its unlawful and wrongful conduct.

255. Plaintiffs and the Class members accordingly are entitled to relief, including restitution and disgorgement of all revenues, earnings, and profits that Jefferson Health obtained because of its unlawful and wrongful conduct.

PRAYER FOR RELIEF

Wherefore, Plaintiffs respectfully ask this Court for an Order:

a. certifying this case as a class action, appointing Plaintiffs as Class Representatives, and appointing Stephan Zouras LLP as Class Counsel;

b. entering judgment for Plaintiffs and the Class members on their ECPA claim and awarding all damages available under 18 U.S.C. § 2520, including equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs;

c. entering judgment for Plaintiffs and the Class members on their breach of contract claim and requiring Jefferson Health to pay all available damages, including the value Jefferson Health received from being able to use individually-identifiable health information intercepted from Jefferson Health's web properties to build more fulsome profiles of Plaintiffs' and the Class members' preferences and traits, and disgorgement of the profits it received from the sale of targeted advertisements based on individually-identifiable health information intercepted from Jefferson Health's web properties and the increased value of revenue it received from Jefferson Health for advertisements placed on Meta's social media platforms following insertion of the Meta's Collection Tools on Jefferson Health's web properties;

d. entering judgment for Plaintiffs and the Class members on their negligence claim and requiring Jefferson Health to pay all available damages, including the value Jefferson Health received from selling or licensing Plaintiffs' and the Class members' personally-identifiable patient health information to Meta and/or sharing this information with Meta, and the value Jefferson Health received from using Plaintiffs' and the Class

members' personally-identifiable patient health information for its own commercial benefit;

e. entering judgment for Plaintiffs and the Class members on their intrusion upon seclusion claim and requiring Jefferson Health to pay all available damages, including injunctive relief requiring Jefferson Health to cease violating their privacy rights without their knowledge or consent and nominal damages of $100 per violation;

f. awarding injunctive relief to Plaintiffs and the Class members that includes an order barring Defendant from any further interception, transmission, or commercial use of Plaintiffs' and the Class members' communications with their doctors and medical office staff on Jefferson Health's web properties absent express notice and informed consent;

g. awarding pre- and post-judgment interest on all damages awarded;

h. awarding recovery of Plaintiffs' reasonable attorneys' fees and reimbursement of their litigation expenses; and

i. awarding such additional relief as justice requires.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Respectfully Submitted,

Dated: October 27, 2023

/s/ *David J. Cohen*
David J. Cohen
STEPHAN ZOURAS, LLP
604 Spruce Street
Philadelphia, PA 19106
(215) 873-4836
dcohen@stephanzouras.com

Ryan F. Stephan (admitted *pro hac vice*)
James B. Zouras (admitted *pro hac vice*)
Teresa M. Becvar (admitted *pro hac vice*)
STEPHAN ZOURAS, LLP
222 W. Adams Street, Suite 2020
Chicago, IL 60606

(312) 233-1550
rstephan@stephanzouras.com
jzouras@stephanzouras.com
tbecvar@stephanzouras.com

Attorneys for Plaintiffs